US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- August 2010 -

This report summarizes general activity as well as updates made to the National Cyber Alert System in August 2010. It includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During August 2010, US-CERT issued 21 Current Activity entries, 4 Technical Cyber Security Alerts, 4 Cyber Security Alerts, 5 weekly Cyber Security Bulletins, and 2 Cyber Security Tips.

Highlights for this month include multiple updates from Microsoft, Adobe, Apple, Cisco, and Google.

Contents

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities presently being reported to US-CERT. The table lists all of the entries posted this month followed by a brief overview of the most significant entries.

Current Activity for August 2010	
August 2	Microsoft Releases Out-of-Band Security Bulletin to Address Shortcut Vulnerability
August 5	Cisco Releases Security Advisory for Firewall Services Module
August 5	Microsoft Releases Advance Notification for August Security Bulletin
August 6	Foxit Releases Foxit Reader 4.1.1.0805
August 10	Microsoft Releases August Security Bulletin
August 11	Adobe Releases Security Update for Flash Player
August 11	Apple Releases Updates for iPhone, iPod touch, and iPad
August 11	Google Releases Chrome 5.0.375.126
August 13	Apple Releases QuickTime 7.6.7
August 16	Cisco IOS Software Vulnerability

Current Activity for August 2010	
August 19	Adobe Releases Security Update for Adobe Reader and Acrobat
August 20	Google Releases Chrome 5.0.375.127
August 20	VideoLAN Releases a Security Advisory for VLC Media Player
August 24	Microsoft Releases Security Advisory
August 25	Adobe Releases Security Bulletin for Shockwave Player
August 25	Apple Releases Security Update 2010-005
August 25	APWG Fax Back Phishing Education Program
August 25	Cisco Releases Advisories for Unified Communications Manager and Unified Presence
August 25	Insecure Loading of Dynamic Link Libraries in Windows Applications
August 31	Cisco Releases Security Advisory for IOS XR Software Border Gateway Protocol
August 31	RealNetworks Releases Update to Address Vulnerabilities in RealPlayer

- Microsoft released multiple updates in July.
  - Security Bulletin MS10-046 addressed a critical vulnerability affecting Microsoft Windows. This vulnerability is due to the failure of Microsoft Windows to properly obtain icons for shortcut files. By convincing a user to display a specially crafted shortcut file, a remote attacker may be able to execute arbitrary code.
  - Microsoft has released Security Advisory 2269637 indicating that it is aware of a remote attack vector for a class of vulnerabilities related to how applications load external dynamic link libraries (DLLs). See the Security Highlights section for further details.
  - The Microsoft Security Bulletin Summary for August 2010 addressed vulnerabilities in Microsoft Windows, Internet Explorer, Office, and Silverlight. These vulnerabilities may allow an attacker to execute arbitrary code or operate with elevated privileges.
- Adobe released updates for Shockwave, Reader, and Acrobat.
  - Flash Player 10.1.82.76 addressed multiple vulnerabilities that may allow an attacker to execute arbitrary code or cause a denial-of-service condition. This vulnerability also affects Adobe Air 2.0.2.12310 and earlier versions. Refer to Adobe Security Bulletin APSB10-16 and US-CERT Vulnerability Note VU#660993 for additional details.
  - Adobe Security Bulletin APSB10-17 addressed multiple vulnerabilities in Reader and Acrobat. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition or execute arbitrary code.
  - Adobe security bulletin APSB10-20 addressed multiple vulnerabilities affecting Shockwave Player 11.5.7.609 and earlier versions. These vulnerabilities may allow an attacker to execute arbitrary code.
- Apple released updates for QuickTime, iOS, and multiple applications.
  - QuickTime 7.6.7 for Windows addressed a vulnerability regarding a stack buffer overflow that exists in QuickTime error logging. By convincing a user to open a specially crafted movie file, a remote attacker could execute arbitrary code or cause a denial-of-service condition. Additional details are provided in Apple article HT4290.

- iOS 4.0.2 for the iPhone and iPod touch and iOS 3.2.2 for the iPad addressed vulnerabilities in the FreeType and IOSurface packages. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or gain system privileges. Additional information regarding the vulnerability affecting the FreeType package can be found in US-CERT Vulnerability Note VU#275247 and Apple article HT4291.
- Apple security update 2010-005 addressed multiple vulnerabilities affecting the ATS, CFNetwork, ClamAV, CoreGraphics, libsecurity, PHP, and Samba applications. These vulnerabilities may allow an attacker to execute arbitrary code, obtain sensitive information, cause a denial-of-service condition, or impersonate hosts within a domain. Refer to Apple article HT4312 for details.

- Cisco released multiple Security Advisories in August.
  - Security Advisory cisco-sa-20100804-fwsm addressed multiple vulnerabilities in the Cisco Firewall Services Module. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition.
  - Security Advisory cisco-sa-20100812-tcp addressed a vulnerability affecting IOS Software Release 15.1(2)T. This vulnerability may allow an attacker to cause a denial-of-service condition by sending a specially crafted packet through normal network traffic.
  - Security Advisory cisco-sa-20100827-bgp addressed a vulnerability in the Cisco IOS XR Software Border Gateway Protocol feature. Exploitation of this vulnerability may result in the continuous resetting of BGP peering sessions, which may cause a denial-of-service condition for affected networks.
  - Cisco released Security Advisory cisco-sa-20100825-cucm and Security Advisory cisco-sa-20100825-cup to address vulnerabilities in Cisco Unified Communications Manager and Cisco Unified Presence. These vulnerabilities affect the processing of Session Initiation Protocol (SIP) messages. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service condition, which could cause an interruption of voice services.

- Google released two updates for Chrome.
  - Chrome 5.0.375.126 for Linux, Mac, and Windows contained an updated version of the Flash plugin, which addresses multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.
  - Later in the month, Google released Chrome 5.0.375.127 for Windows, Mac, and Linux to address multiple vulnerabilities that may allow an attacker to execute arbitrary code, cause a denial-of-service condition, or conduct spoofing attacks. Additional information can be found in the Google Chrome Releases blog entry.

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for August 2010	
August 10	TA10-222A Microsoft Updates for Multiple Vulnerabilities
August 11	TA10-223A Adobe Flash and AIR Vulnerabilities
August 19	TA10-231A Adobe Reader and Acrobat Vulnerabilities
August 26	TA10-238A Microsoft Windows Insecurely Loads Dynamic Libraries

Cyber Security Alerts

Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

Cyber Security Alerts (non-technical) for August 2010	
August 10	SA10-222A Microsoft Updates for Multiple Vulnerabilities
August 11	SA10-223A Adobe Flash and AIR Vulnerabilities
August 12	SA10-224A Apple Updates iOS for Multiple Vulnerabilities
August 19	SA10-231A Adobe Reader and Acrobat Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology's (NIST's) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / US-CERT. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for August 2010
SB10-214 Vulnerability Summary for the Week of July 26, 2010
SB10-221 Vulnerability Summary for the Week of August 2, 2010
SB10-228 Vulnerability Summary for the Week of August 9, 2010
SB10-235 Vulnerability Summary for the Week of August 16, 2010
SB10-242 Vulnerability Summary for the Week of August 23, 2010

A total of 380 vulnerabilities were recorded in the NVD during August 2010.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users.

Cyber Security Tips for August 2010	
August 12	ST05-013 Guidelines for Publishing Information Online
August 25	ST05-014 Real-World Warnings Keep You Safe Online

Security Highlights

Microsoft Windows Insecurely Loads Dynamic Libraries

Due to the way Microsoft Windows loads dynamically linked libraries (DLLs), an application may load an attacker-supplied DLL instead of the legitimate one, resulting in the execution of arbitrary code. Microsoft has released a security advisory indicating that it is aware of this remote attack vector. If an application does not securely load DLL files, an attacker may be able to cause the application to load an arbitrary library. By convincing a user to open a file from a location that is under an attacker's control, such as a USB drive or network share, a remote attacker may be able to exploit this vulnerability. Exploitation of this vulnerability may result in the execution of arbitrary code or elevation of privileges.

At this time, US-CERT is aware of reports of publicly available exploit code for this vulnerability. US-CERT encourages users and administrators to review Microsoft security advisory 2269637 and consider implementing the workarounds listed in the document. Please note that these workarounds may reduce the functionality of the affected systems. Workarounds include the following:

- Disable the loading of libraries from WebDAV and remote network shares.
- Disable the WebClient service.
- Block TCP ports 139 and 445 at the firewall.

Any application running on the Microsoft Windows platform that uses DLL files may be affected and may require patches. Whether or not an application is vulnerable depends on how it specifically loads a DLL. Please see the Vendor Information section of Vulnerability Note VU#707943 for information about specific vendors. Microsoft Knowledge Base article KB2264107 describes an update, which provides a registry key that can prevent Windows from searching the current working directory for DLL files.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or learn more about cyber security, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xCB0CBD6E
PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E
PGP Key: https://www.us-cert.gov/pgp/info.asc